UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/026,043	10/25/2001	Huayan A. Wang	1190	8635

83694 7590 12/22/2008

Fay Kaplun & Marcin, LLP/ Motorola
150 Broadway Suite 702
New York, NY 10038

EXAMINER	
KIM, JUNG W	
ART UNIT	PAPER NUMBER
2432	
MAIL DATE	DELIVERY MODE
12/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/026,043
Filing Date: October 25, 2001
Appellant(s): WANG ET AL.

Oleg F. Kaplun
Registration Number 45,559
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 9/30/08 appealing from the Office action mailed 5/14/08.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

20020174335	Zhang et al.	11-2002
6760444	Leung	7-2004
6452910	Vij et al.	9-2002
6178506	Quick, Jr.	1-2001
5732350	Marko et al.	3-1998
5408683	Ablay et al.	4-1995

Rigney et al; RFC 2138; April 1997

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-3, 6, 10, 11 and 15-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung USPN 6,760,444 (hereinafter Leung) in view of Marko et al. USPN 5,732,350. (hereinafter Marko)

As per claim 1, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of:

a. generating, by an authentication server of the network, authentication data associated with the roaming device (col. 7:35-36);

b. sending, by the authentication server, the authentication data to an access point of the network, the access point being connected to the authentication server(7:38-50); and

c. when the roaming device roams to a particular access point, determining if the particular access point has authentication data associated with the roaming device, using the authentication data to locally authenticate the roaming device at the particular access point if the determination is positive, or carrying out the authentication process at the authentication server if the determination is negative. (7:50-67)

Leung does not disclose sending the authentication data to a plurality of access points and storing the authentication data in the plurality of access points, such that the roaming device is locally authenticated at a particular access point of the plurality of access points. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a plurality of access points and locally store the authentication data in the plurality of access points. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 1.

As per claim 2, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the step of storing the authentication data in a memory arrangement of each of the access points. See Leung, col. 7:50-67; Marko, 7:24-56.

As per claim 3, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. Leung does not expressly teach the authentication data is encrypted. However, it is notoriously well known in the art that authentication data transmitted in the clear is susceptible to sniffing attacks. To prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the authentication data to be transmitted securely to prevent the data from being stolen as known to one of ordinary skill in the art. The aforementioned cover the limitations of claim 3.

As per claim 6, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the preliminary steps of determining if the particular access point has authentication data associated with the roaming device; if the determination is positive, proceed to the step of using the authentication data to locally authenticate the roaming device at the particular access point; and if the determination is negative, proceed to the step of generating, by an authentication server of the network, authentication data associated with the roaming device. Leung, col. 7:10-31; 7:56-8:8.

As per claim 10, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of:

d. connecting the roaming device with an authentication server upon a contact of the roaming device with a first access point of the network; authenticating the roaming device with the authentication server if the access point has no authentication data associated with the roaming device; generating authentication data for the roaming device; distributing, by the authentication server, the authentication data to the first access point of the network; and locally authenticating the roaming device upon a contact with the first access point using the distributed authentication data. Col. 7:35-67.

Leung does not disclose sending the authentication data to a second access point and storing the authentication data in the second access point, then locally authenticating the roaming device upon a contract with the second access point using the distributed authentication data. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a second access point and store the authentication data in the second access point, then locally authenticate the roaming device upon a contract with the second access point using the distributed authentication data. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 10.

As per claim 11, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the method further comprising the step of authenticating the roaming device with the authentication server if the local authentication of the roaming device fails. Leung, col. 7:10-31; 7:56-8:8.

As per claim 15, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the authentication server is a remote authentication dial-in user server. Leung, col. 7:1-5.

As per claim 16, Leung discloses a system for authenticating a roaming device with a network, comprising:

e. an authentication server connected to the network; and first and second access points connected to the authentication server, the first and second access points being capable of communicating with the roaming device, each of the first and second access points including a memory arrangement capable of storing authentication data corresponding to the roaming device, wherein the authentication server sends the authentication data to the first access point upon an initial authentication procedure of the roaming device with the first access point when the first access point has no authentication data associated with the roaming device, and wherein the first access point authenticates the roaming device upon a contact of the roaming device with the first access point. Col. 7:35-67.

Leung does not disclose sending the authentication data to a second access point and storing the authentication data in the second access point, then locally authenticating the roaming device upon a contract with the second access point using the distributed authentication data. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with a based station in this cell, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a new base station within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to send the authentication data to a second access point and store the authentication data in the second access point, then locally authenticate the roaming device upon a contract with the second access point using the distributed authentication data. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned covers the limitation of claim 16.

As per claim 17, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the second access point authenticates the roaming device with the authentication server if the authentication data is not found in the memory arrangement of the second access point. Leung, col. 7:10-31; 7:56-8:8.

As per claim 18, the rejection of claim 16 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the second access point authenticates the roaming device with the authentication server if the local authentication of the roaming device at the second access point fails. Leung, col. 7:10-31; 7:56-8:8.

Claims 4 and 5 are rejected under 35 USC 103(a) as being unpatentable over Leung in view of Marko, and further in view of Ablay et al. USPN 5,408,683. (hereinafter Ablay)

As per claim 4, the rejection of claim 3 under 35 USC 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. Leung does not expressly disclose using prediction algorithms to anticipate where the roaming device will roam to determine to which access points to send the encrypted authentication data. Ablay discloses a method of tracking subscribers in a networked radio communications system having a plurality of trunked communication networks using location information of the subscribers to anticipate a roaming unit's location to reduce the number of registrations and de-registrations of the roaming unit. Col. 5:19-60; 6:26-57. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Ablay with the invention of Leung and Marko to use prediction algorithms to anticipate where the roaming device will roam to determine to which access points to send the encrypted authentication data. One would be motivated to do so to reduce the transmission overhead in keeping track of roaming subscribers. Ablay, 3:30-37. The aforementioned cover the limitations of claim 4.

As per claim 5, the rejection of claim 4 under 35 USC 103(a) as being unpatentable over Leung in view of Marko and Ablay is incorporated herein. In addition, the limitation of sending the encrypted authentication data to all the access points is an obvious enhancement in view of the teaching of Ablay that a mobile unit's registration is maintained at all access points in the anticipated probable locations of the mobile unit. Ablay, col. 5:19-26. The aforementioned cover the limitations of claim 5.

Claims 7, 8 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko, and further in view of Vij et al. USPN 6,452,910. (hereinafter Vij)

As per claim 7, the rejection of claim 6 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. (supra) In addition, the step of using the authentication data to locally authenticate the roaming device further comprises reassociating the roaming device with the particular access point of the access points by providing identification information. Leung, col. 7:10-13. However, Leung only discloses that the roaming device provides identification, and does not disclose that an exchange occurs between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points utilizing a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. Col. 11:1-7. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants belong to the same local network. Vij, ibid. The aforementioned cover the limitations of claim 7.

As per claim 8, the rejection of claim 7 under 35 U.S.C. 103(a) is incorporated herein. In addition, the reassociating step further includes the substeps of: searching a memory arrangement of the particular access point for the authentication data associated with the roaming device; and if the authentication data is found, performing a mutual authentication procedure between the roaming device and the particular access point. Leung, col. 7:10-31; 7:56-8:8; Vij, 11:1-7.

As per claim 13, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, Leung discloses the locally authenticating step further includes the substeps of: providing identification data by the roaming device to the second access point; and correlating the identification data with the distributed authentication data. Col. 7:10-13. However, Leung only discloses that the roaming device provides identification, and does not disclose exchanging identification between the roaming device and access points to reassociate. Vij discloses a management means for wireless access points wherein wireless devices are mutually authenticated with access points using a common link key to verify that the wireless device is authorized to access the access point, and to ensure that the access point is the intended receiver. Col. 11:1-7. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the reassociating to include a mutual authentication between the roaming device and the access point, since it is desirous to verify that the participants of a transmission belong to the same local network. Vij, ibid. The aforementioned cover the limitations of claim 13.

Claims 9, 12 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko, and further in view of Zhang et al. US Patent Application no. 20020174335 (hereinafter Zhang); RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

As per claim 9, the rejection of claim 1 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, the generating step further includes the steps of: receiving an authentication request from the roaming device; determining that the roaming device can be granted access to network services. Leung, col. 7:11-8:12. Leung does not expressly teach generating an encrypted session key associated with the roaming device in the authentication server; wherein the authentication request is encrypted. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user. (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made to generate an encrypted session key associated with the roaming device in the authentication server; wherein the authentication request is encrypted. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claim 9.

As per claims 12 and 14, the rejection of claim 10 under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Marko is incorporated herein. In addition, Leung discloses the use of RADIUS protocol to authenticate the user with an authentication server, but Leung does not expressly disclose the distribution step further includes the substep of distributing an encrypted session key to the first and second access points, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm

MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the distribution step to further include the substep of distributing an encrypted session key to the first and second access points, the method further comprising the steps of establishing a shared secret encryption between the authentication server and the first and second access points. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claims 12 and 14.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang; RFC 2138 is incorporated to illustrate inherent properties of the RADIUS protocol.

As per claim 19, Leung discloses a method for authenticating a roaming device with a network, comprising the steps of: with an authentication server, receiving an authentication request from a roaming device if the access point connected with the roaming device has no authentication data associated with the roaming device, sending the authentication data to an access point of the network, and utilizing the authentication data to authenticate the roaming device at the access point. Leung does not disclose the request being encrypted with a first shared code; generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point. Zhang discloses an authentication procedure for mobile devices designed by Cisco wherein a roaming user is authenticated via an access point, and uses the RADIUS protocol to authenticate the user to an authentication server. Upon, authentication, an encrypted session key is delivered from the authentication server to the access point and the user (pg. 3, paragraphs 44-46; RFC 2138, pg. 4, last sentence, section 2, the password is encrypted using a method based on the RSA message digest algorithm MD5) Further, it is notoriously well known that authentication data transmitted in the clear is susceptible to sniffing attacks; to prevent authentication data from being stolen, these values are typically encrypted using a shared secret between the sender and receiver. For example, in the RADIUS protocol, a password transmitted from a client to an authentication server is hidden using a shared secret. Hence, it would be obvious to one of ordinary skill in the art at the time the invention was made for the request to be encrypted with a first shared code; generating a session key associated with the roaming device; sending the session key to an access point of the network, the session key being encrypted with a second shared code; and utilizing the session key to authenticate the roaming device at the access point, and to encrypt data exchanged between the roaming device and the access point. One would be motivated to do so to securely transmit data as reflected in the RADIUS protocol and the Cisco authentication procedure. The aforementioned cover the limitations of claim 19.

Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang, and further in view of Marko.

As per claim 20, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. Leung does not disclose the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point. Marko discloses a method for registering a mobile station among a plurality of base stations based upon a dynamic algorithm. When a mobile station approaches a cell where the mobile station is not yet registered, the mobile station registers with this station, whereupon a network controller automatically registers the mobile station with all base stations within the group defined by the cell grouping level. Col. 7:24-57; 8:51-9:28. This enables the mobile station to roam among a cell grouping without registering each time the mobile moves to a cell within the grouping. It would be obvious to one of ordinary skill in the art at the time the invention was made to include the step of sending the encrypted session key to a further access point of the network to authenticate the roaming device at the further access point. One would be motivated to do so to reduce user registration traffic. Marko, col. 1:58-65; 2:36-40. The aforementioned cover the limitations of claim 20.

Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Leung in view of Zhang, and further in view of Quick, Jr. USPN 6,178,506 (hereinafter Quick ‘506).

As per claim 21, the rejection of claim 19 under 35 U.S.C. 103(a) is incorporated herein. In addition, Leung in view of Zhang discloses the method further comprising the steps of: generating a first key of the session key to perform authentication of the roaming device at the access point; and generating a second key of the session key to encrypt data exchanges between the roaming device and the access point. See Leung, 7:50-61; see Zhang, paragraph 45. Leung does not expressly teach the first key as being different from the second key. Quick ‘506 discloses an authentication method wherein a first portion of a session key is used for authentication and a second portion of the session key is used for encryption. Since, the session key is larger then the required byte size necessary for authentication, the portion not used for authentication is used for encryption. Col. 5:38-50. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made for the first key generated from the session key to perform authentication and the second key generated from the session key to perform encryption to be different keys, since the protocols for authentication and encryption typically require different length keys. Quick ‘506, 5:45-50. The aforementioned cover the limitations of claim 21.

(10) Response to Argument

Appellant's arguments are not found to be persuasive because of two reasons: First, Appellant only provides a conclusionary statement that the secondary reference does not overcome the deficiency of the primary reference. See Appeal Brief, pg. 7, line 10. Conclusionary statements, by themselves, do not establish a rationale or argument against a 103(a) rejection because they are mere statements; nor do they provide any factual support for a claim that a rejection based on the combined teachings of two references does not properly render the claimed invention obvious.

Second, Appellant's arguments are predicated on an interpretation of Leung that is not the basis for the 103(a) rejection. In interpreting the prior art rejections, Appellant maps a home agent of Leung with the claimed authentication server. Appeal Brief, pg. 6, last sentence. However, as applied in the rejections, it is indicated that Leung expressly discloses the use of a centralized security database (supra; see Leung, fig. 6, reference no. 602), which anticipates the claimed authentication server limitation, and a plurality of home agents (see reference nos. 506-514), which anticipates the plurality of access points as defined in claim 1.

In particular, Leung discloses a mobile authentication method and apparatus, having a centralized security database as a source for security association data, and several access points by which a mobile device can authenticate. Fig. 6, col. 6, lines 18-28. In Leung's invention, when a mobile device approaches an access point, an authentication request is sent from the mobile device to the access point. If the access point is a home agent, this authentication request is submitted to the centralized database, whereupon the centralized database replies with an authentication response packet, which includes a security association. If the access point is a foreign agent, the request is first forwarded to the home agent, and then to the centralized database. Col. 7, lines 23-50; col. 8, lines 4-25. In order to reduce excessive authentication requests to the centralized database, Leung's invention discloses an embodiment where security association data for a mobile device that is retrieved from the centralized security database is cached at the home agent. Col. 7, lines 50-67. Hence, this portion of Leung expressly discloses performing the authorization step at the home agent rather than the centralized database, if the home agent has cached security association data for the mobile device.

Marko discloses a method and system for registering a mobile device with several base stations simultaneously thereby reducing registration traffic between the base stations and the network controller. In particular, when a mobile device first roams into a cell (service area) where the device has not registered with the base station servicing the cell, the device first registers with this base station, whereupon the network controller automatically registers the mobile device with other base stations identified by a cell grouping level by providing registration information for the mobile device to these other base stations. Col. 7, lines 24-57; col. 8, line 51-col. 9, line 28. This feature enables the mobile device to roam among the service areas within a defined cell group without requiring the mobile device to register each time the mobile device moves to a new base station within the cell group.

Hence, in view of the prior art, although the invention of Leung does not teach sending the authentication data for a mobile device to a plurality of access points and storing the authentication data in the plurality of access points as defined in the limitations of claim 1, Marko expressly discloses sending registration data to access points within a cell grouping, once a mobile device registers with one of the access points in the cell group. Ibid. Furthermore, Marko expressly teaches that such a feature is an improvement in the art because it reduces registration traffic for wireless registration of mobile devices. Col. 9, lines 32-35. Therefore, it would be obvious to one of ordinary skill in the art at the time the invention was made to modify the Leung invention with the following steps: sending the authentication data to a plurality of access points, whereby when the roaming device roams to a particular access point; if the particular access point has authentication data associated with the roaming device, the device is authenticated locally; otherwise, the roaming device is authenticated by the authentication server.

For these reasons, it is respectfully submitted that Leung in view of Marko suggest the method of claim 1.

Appellant's arguments against the rejections of the remaining claims are based on the arguments against the rejection of claim 1. See Appeal Brief, pgs. 7-13. Hence, Appellants arguments for these claims are found to be deficient for the same reasons outlined above.

For the above reasons, it is believed that the rejections should be sustained.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

Respectfully submitted,

/Jung Kim/
Primary Examiner, Art Unit 2432

Conferees:

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2432